IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF FLORIDA TALLAHASSEE DIVISION

UNITED STATES OF AMERICA

Case No: 4:16cr43-MW

VS.

ANTONIO FUGUET

STATEMENT OF FACTS

The defendant admits that if this case were to proceed to trial, the government could prove the following beyond a reasonable doubt.

On October 16, 2015, the Leon County Sheriff's Office Internet Crimes Against Children (ICAC) unit was conducting an investigation of the ARES peer-to-peer (P2P) network. The unit found approximately 25 files of suspected child pornography (CP) on a computer with the IP address of 73.48.108.78. The unit continued to monitor IP address 73.48.108.78, and the number of CP files rose to 57. Among the files that the ICAC investigators were able to associate with IP address 73.48.108.78 was a file depicting a pre-pubescent nude female lying on a bed with vagina exposed in a lewd manner. The child masturbates and then performs oral sex on an adult male penis.

Investigators learned that IP address 73.48.108.78 was issued by Comcast.

On October 23, 2015, investigators obtained a State of Florida subpoena for

FILED IN OPEN COURT THIS

CLERK, U.S. DISTRICT COURT, NORTH, DIST, FLA. information on IP address 73.48.108.78. The information obtained from the subpoena indicated that on October 16, 2015, the IP address was assigned to an address in Tallahassee, Florida.

Investigators obtained a State of Florida search warrant on December 3, 2015, for the address provided by Comcast, which they executed on December 4, 2015. During the search, agents discovered that the defendant, Antonio Fuguet and two other individuals were living at the residence.

The defendant was interviewed in Spanish. The interview was audio recorded, and the defendant was read his *Miranda* rights in Spanish and waived them. He indicated that he used file sharing and admitted to downloading and viewing child porn. He admitted to owning computers in the residence, and three laptops were found in his room. He indicated that the Toshiba laptop was his primary computer and that it was password protected. The defendant said that he was the only one who knows the password. He also indicated that no one else in the residence uses his computers. He admitted to downloading videos of children engaged in sexual activity. The defendant said that he would download them at night, watch them and delete them. He said he would do it because he was "curious" and "wanted to see." The defendant admitted using search terms such as "pthc" and "kid." He estimated that he had downloaded no more than 20 total videos.

During the search warrant, officers seized a HP Pavilion Laptop Model DV2000 (serial # 2CE7130DRZ), a Toshiba Satellite Model C55-B5101 (serial # 3F018158P), and other electronic items. A preliminary exam on the scene revealed CP on the Toshiba laptop and the HP Pavilion Model DV2000 laptop. A full forensic examination was then conducted and revealed numerous images of CP within the \USERS\ANTONIOJOSE\ directory on the Toshiba, and the \USERS\USER\ directory on the HP laptop.

The forensic examination was consistent with the defendant's claim that he was downloading then deleting files from his hard drive. Three partial videos were recovered from the HP laptop and 8 partial videos were recovered from the Toshiba. All of these 11 videos would play and contained CP. The 3 videos from the HP laptop all involved toddler-age females, clearly under 12 years old. Two of videos show vagina penetration of the children by an adult male's penis, and the other video shows digital penetration. 237 images were recovered from the Thumbcache database on the Toshiba laptop. Many of the photographs involve children under the age of 12. Agents also identified images on the Toshiba laptop from the "Vicky" series showing a child bound and masked.

The ARES program records for the defendant's computer show that additional files had been downloaded, which were subsequently deleted. The examiners were also able to determine the dates that the defendant accessed the ARES network and the files that he downloaded. The defendant accessed the network using the same user name and the same IP address on multiple dates between December 26, 2014, and October 16, 2015. These records show 19 video downloads.

The child pornography images downloaded by the defendant were shipped and transported in interstate commerce through the ARES peer-to-peer computer network.

ELEMENTS

Receipt of Child Pornography - 18 U.S.C. 2252A(a)(2)

- (1) That the Defendant knowingly received an item or items of child pornography;
- (2) That such items of child pornography had been shipped or transported in interstate or foreign commerce including by computer; and

(3) That at the time of such receipt the Defendant believed that such items contained child pornography.

,	CHRIŞTOPHER P. CANOVA
	United States Attorney
1-5-2017	
Date	GARY MILLIGAN
	District of Columbia Bar No. 484813
	Assistant United States Attorney
	Northern District of Florida
	111 N. Adams, Fourth Floor
	Tallahassee, Florida 32301
	850-942-8430
	Gary.Milligan@usdoj.gov
1/5/17 Date	JOSEPH F. DEBELDER Attorney for Defendant
1/5/17 Date	Antonio J. Fraguet L ANTONIO FUGUET